| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sisestage siia registreeritud juriidilise isiku nimi | | | | | | | |
| Dokumendi number:<br>P27S | | | | | Dokumendi pealkiri:<br>**Pilveteenuste kasutamise poliitika** | | | | | | | |
| Versioon:<br>1.0 | | Jõustumiskuupäev:<br>01.01.2025 | | | Dokumendi omanik: | | | | | | | |
| X | Poliitika | | Standard | | Protseduur | | Vorm | | Register | | Muu | |

| **Muudatuste ajalugu** | | | | |
|---|---|---|---|---|
| **Muudatuse number** | **Muudatuse kuupäev** | **Muudatused** | **Läbi vaadanud** | **Protsessi omanik** |
| | | | | |
| | | | | |

| **Kinnitused** | | | |
|---|---|---|---|
| **Nimi** | **Ametikoht** | **Kuupäev** | **Allkiri** |
| | | | |
| | | | |

Kooskõla standardite ja õigusaktidega

| Standard/õigusakt | Punkt/artikkel | Kommentaar |
|---|---|---|
| ISO/IEC 27001:2022 | Punkt 8 | |
| ISO/IEC 27002:2022 | Kontrollimeetmed 5.23–5.25 | |
| NIST SP 800-53 Rev. 5 | AC-20, SC-12, SC-13, SR-5 | |
| ELi isikuandmete kaitse üldmäärus (GDPR) | Artikkel 28, 32 ja V peatükk | |
| ELi NIS2 | Artiklid 21(2)(f), (i) | |
| ELi DORA | Artiklid 5(2), 28 | |
| COBIT 2019 | DSS01, DSS05, BAI04 | |

**1. Eesmärk**

1.1 Käesolev poliitika määratleb, kuidas pilveteenuseid võib organisatsioonis turvaliselt kasutada. See tagab, et pilves töödeldavad või säilitatavad andmed on kaitstud, juurdepääs on kontrollitud ning riske juhitakse asjakohaselt.

1.2 See aitab VKE-del täita õiguslikke kohustusi ja klientide ootusi tundliku teabe kaitsel, andmeleket ennetada ning pilvekeskkonnas tekkivaid riske tõhusalt hallata ilma ettevõtte mastaabis taristut vajamata.

1.3 Käesolev poliitika toetab ISO/IEC 27001 sertifitseerimist, GDPRi nõuetele vastavust ja tarneahela usaldusväärsust kõigi kolmandate osapoolte pilveteenuste järjepideva juhtimise kaudu.

**2. Kohaldamisala**

**2.1 Käesolev poliitika kohaldub järgmisele:**

2.1.1 kõik pilvepõhised teenused, mida kasutatakse ettevõtte andmete salvestamiseks, töötlemiseks või edastamiseks;

2.1.2 kõik töötajad, töövõtjad ja teenuseosutajad, kes kasutavad organisatsiooni nimel pilvetööriistu;

2.1.3 tasuta ja tasulised pilvelahendused, sealhulgas e-posti platvormid, dokumendijagamise lahendused, SaaS-tööriistad, varundusplatvormid, videokonverentsilahendused ja kliendiplatvormid;

2.1.4 kõik seadmed (lauaarvutid, mobiiltelefonid, tahvelarvutid), mille kaudu kasutatakse ettevõtte teabele juurdepääsuks pilverakendusi.

**2.2 See hõlmab muu hulgas järgmist:**

2.2.1 Microsoft 365, Google Workspace, Dropbox Business;

2.2.2 Zoom, Microsoft Teams, Google Meet;

2.2.3 AWS, Azure, GCP;

2.2.4 pilvepõhised varundus- ja katastroofitaaste tööriistad;

2.2.5 ühiskaustad või rakendused, mida kasutatakse arvelduseks, projektijuhtimiseks või kliendisuhtluseks.

**3. Eesmärgid**

3.1 Ennetada heakskiitmata pilveteenuste loata või kõrge riskiga kasutamist.

3.2 Tagada, et pilves säilitatavad tundlikud või reguleeritud andmed on kaitstud asjakohaste tehniliste ja korralduslike meetmetega.

3.3 Määratleda selged rollid pilveteenuste heakskiitmisel, konfigureerimisel, seirel ja kasutuselt kõrvaldamisel.

3.4 Kontrollida andmevooge ning tagada pilves säilitatava teabe suhtes säilitamis-, kustutamis- ja andmekaitsekohustuste täitmine.

3.5 Vähendada sõltuvust isiklikest kontodest ja järelevalveta tööriistadest, nõudes kõigi ärilistel eesmärkidel kasutatavate pilvesüsteemide eelnevat heakskiitu.

3.6 Täita ISO/IEC 27001:2022, GDPRi, NIS2 ja DORA nõuded väliste pilveteenustest sõltuvuste haldamisel.

**4. Rollid ja vastutused**

**4.1 Tegevjuht**

4.1.1 kiidab heaks kõigi uute pilveteenuste kasutuselevõtu;

4.1.2 vaatab läbi pilveteenuse osutajate ja teenuseliikidega seotud riskid;

4.1.3 tagab poliitika järgimise ja teeb järelevalvet erandite üle otsustamise üle.

**4.2 Väline IT-teenuseosutaja või tehniline tugi**

4.2.1 hindab ja rakendab pilveteenuste turvalist konfiguratsiooni;

4.2.2 seadistab kontod, juurdepääsukontrolli ja varunduse;

4.2.3 jälgib paroolide, MFA ja turvaseadistuste nõuete täitmist.

[ ... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ... ]

**9. Läbivaatamise ja ajakohastamise nõuded**

9.1 Tegevjuht peab käesoleva poliitika koostöös välise IT-teenuseosutajaga vähemalt kord aastas läbi vaatama.

**9.2 Ametlik läbivaatus tuleb teha ka järgmistel juhtudel:**

9.2.1 pärast pilveteenustega seotud turvaintsidenti (nt rikkumine, andmekadu);

9.2.2 uue suurema pilveplatvormi kasutuselevõtul;

9.2.3 kui õiguslikud või regulatiivsed nõuded muutuvad (nt GDPRi, NIS2 või DORA muudatused);

9.2.4 kui seiretegevused toovad esile väärkasutuse või uued riskid.

**9.3 Tegevjuht peab tagama, et:**

9.3.1 pilveteenuste registrit ajakohastatakse uute või kasutuselt kõrvaldatud teenustega;

9.3.2 õiguslikud ja andmekaitsenõuded on jätkuvalt täidetud;

9.3.3 kõik muudatused tehakse asjaomastele kasutajatele ja sidusrühmadele teatavaks.

9.4 Arhiveeritud versioone tuleb säilitada turvaliselt ning poliitika varasemaid versioone tuleb käsitleda kooskõlas organisatsiooni poliitikaga P14S – Andmete säilitamise ja kõrvaldamise poliitika.

**10. Seotud poliitikad ja seosed**

**10.1 Käesolevat poliitikat tuleb rakendada koostoimes järgmiste VKEdele kohandatud infoturbepoliitikatega:**

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: määratleb vastutuse pilveteenuste heakskiitmisel ja teenuseosutajate suhete haldamisel.

10.1.2 P4S – Juurdepääsukontrolli poliitika: toetab pilveplatvormide jaoks nõutavat turvalist sisselogimist, seansihaldust ja juurdepääsuõiguste tühistamist.

10.1.3 P14S – Andmete säilitamise ja kõrvaldamise poliitika: reguleerib, kuidas pilvepõhiseid andmeid varundatakse, säilitatakse ja kustutatakse kooskõlas õiguslike kohustustega.

10.1.4 P17S – Andmekaitse ja privaatsuspoliitika: tagab, et pilveteenustes säilitatavaid isikuandmeid töödeldakse kooskõlas GDPRi põhimõtetega.

10.1.5 P30S – Intsidentidele reageerimise poliitika: sätestab korrastatud protseduurid pilveturbe intsidentidele reageerimiseks, sealhulgas tõendusmaterjali kogumiseks ja väliseks teavitamiseks.

10.2 Need poliitikad tagavad koos, et pilveteenuste kasutamine on turvaline, nõuetele vastav ja talitluspidev.

## 11. Viitestandardid ja raamistikud

### 11.1 ISO/IEC 27001

11.1.1 Punkt 8.1 – nõuab, et organisatsioon rakendaks andmekäitluse operatiivseid kontrollimeetmeid, sealhulgas pilvepõhiste süsteemidega seotud kontrollimeetmeid.

### 11.2 ISO/IEC 27002

11.2.1 Kontrollimeede 5.23 – nõuab pilveteenuste ja kolmandate osapoolte SaaS-tööriistade kasutamise juhtimist.

11.2.2 Kontrollimeede 5.24 – nõuab määratletud pilveteenuste kasutamise poliitikat, mis on kooskõlas riski- ja regulatiivsete nõuetega.

11.2.3 Kontrollimeede 5.25 – nõuab, et organisatsioon tagaks pilvekeskkondade turbekontrollide vastavuse organisatsiooni vajadustele.

### 11.3 NIST SP 800-53 Rev. 5

11.3.1 AC-20 – nõuab väliste süsteemide, näiteks pilveteenuste, kasutamiseks ametlikke kasutuspoliitikaid.

11.3.2 SC-12, SC-13 – käsitlevad andmete krüptimist pilvekeskkondades nii edastamisel kui ka puhkeolekus.

11.3.3 SR-5 – hõlmab tarneahela pilve- ja kolmandate osapoolte riskide kontrollimeetmeid.

### 11.4 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679)

11.4.1 Artikkel 28 – nõuab, et andmetöötlejana tegutsevad pilveteenuse pakkujad järgiksid siduvaid lepingulisi kohustusi.

11.4.2 Artikkel 32 – nõuab pilvepõhise andmetöötluse jaoks tehnilisi ja korralduslikke meetmeid.

11.4.3 V peatükk – keelab pilves säilitatavate isikuandmete loata rahvusvahelised edastused.

### 11.5 ELi NIS2 direktiiv (2022/2555)

11.5.1 Artikkel 21(2)(f), (i) – nõuab, et olulised ja tähtsad üksused rakendaksid asjakohaseid poliitikaid pilveteenuste turbe ja tarneahela kontrolli jaoks.

### 11.6 ELi DORA (2022/2554)

11.6.1 Artikkel 5(2) – nõuab, et finantssektori VKEd integreeriksid pilveturbe oma IKT-riskide juhtimise raamistikku.

11.6.2 Artikkel 28 – kehtestab kriitiliste kolmandatest osapooltest IKT-teenuseosutajate, sealhulgas pilveteenuse osutajate, järelevalvereeglid.

### 11.7 COBIT 2019

11.7.1 DSS01 – „Operatsioonide juhtimine“ käsitleb pilveteenuste operatiivset terviklikkust.

11.7.2 DSS05 – „Turbeteenuste juhtimine“ hõlmab pilvespetsiifilisi kaitsemeetmeid ja seiret.

11.7.3 BAI04 – „Käideldavuse ja mahu juhtimine“ tagab talitluspidevuse ja toimivuse pilvekeskkondades.